**UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| **IN THE MATTER OF THE SEARCH OF:**<br><br>**The Offices of Tiversa, located at 606 Liberty Avenue, Pittsburgh, PA 15222** | **UNDER SEAL**<br><br>**Mag. No. 16-180M Amended** |

**AFFIDAVIT IN SUPPORT OF A SUPPLEMENTAL APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Mosi Forde, a Special Agent for the United States Department of Health and Human Services ("HHS"), Office of Inspector General ("OIG"), Office of Investigations ("OI"), Digital Investigations Branch ("DIB"), Computer Crimes Unit ("CCU"), being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of a supplemental application under Rule 41 of the Federal Rules of Criminal Procedure for an amended warrant to search the premises known as the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, Pennsylvania (hereinafter, the "SUBJECT PREMISES"), as further described in Attachment A, for the items described in Attachment B, that is, evidence, information relating to, contraband, fruits, or instrumentalities of the following criminal violations: 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements).

2. On February 29, 2016, the Honorable Robert C. Mitchell, United States Magistrate Judge, issued a search warrant, No. 16-180M, attached hereto as Exhibit 1 and hereby incorporated fully by reference ("the Warrant"), authorizing a search of the SUBJECT PREMISES during the daytime, between 6:00 a.m. and 10:00 p.m., based upon an affidavit, attached hereto as Exhibit 2 and hereby incorporated fully by reference. On March 1, 2016, at 6:00 a.m., law enforcement agents, including your affiant, commenced the execution of the Warrant upon the SUBJECT PREMISES. Between 6:00 a.m. and about 5:00 p.m., agents executing the warrant collected numerous assorted documents deemed to be within the scope of the Warrant and imaged multiple electronic media and digital devices. Approximately 30 law enforcement agents participated in the execution of the search warrant upon the SUBJECT PREMISES.

3. Agents executing the Warrant commenced imaging of the servers on the SUBJECT PREMISES by about 7:30 a.m. today, March 1, 2016. However, upon examination of the servers to be imaged, within the scope of the Warrant, executing agents determined that the hardware configuration of the servers, including the data transfer speeds, did not permit efficient and expeditious imaging of the servers. Executing agents nevertheless attempted, within the scope of the Warrant, to image the servers, which contained some 700 terabytes of information. By approximately 1:00 p.m., it became evident to the executing agents that it was going to be extremely difficult to complete the imaging of the servers within the hours of 6:00 a.m. and 10:00 p.m. as authorized by the Warrant. Agents then attempted to expedite the imaging by examining the directories and folders within the servers to try to reduce the volume of information to be copied. However, the configuration and organization of the content of the

servers rendered on-site attempts to identify all of the information that was seizable within the scope of the Warrant impracticable.

4. Despite executing agents' best efforts to complete the imaging of the contents of the servers, within the scope of the Warrant, it appeared to me and other agents assisting me in the execution of the Warrant that the amount of data remaining to be imaged from the servers at approximately 5:30 p.m., combined with the limited data transfer speeds, output options, and overall hardware configuration, rendered completion of the execution of the Warrant within the daylight hours of 6:00 a.m. to 10:00 p.m., at best unlikely and at worst, impossible.

5. Further, it is not feasible for the executing agents to remove the servers from the SUBJECT PREMISES to be examined off site because such removal would necessitate recreating the same network topography and hard drive configuration at an offsite location which would also be technologically extraordinarily difficult to achieve, even if possible. Moreover, removal of the servers could result in Tiversa's loss of the use of its servers for some prolonged period of time, resulting in a substantial disruption to its business operations.

6. Finally, if imaging were to cease this evening, March 1, 2016, at 10:00 p.m. and recommence at 6:00 a.m. tomorrow morning, the entire imaging process would have to begin anew and, thus, the executing agents would face the same dilemma of not being able to complete the search before 10:00 p.m. tomorrow, March 2, 2016.

7. For all of the foregoing reasons, I respectfully submit that it is necessary that law enforcement continue to execute the Warrant past 10:00 p.m. until such execution is complete and all the data within the scope of the Warrant is imaged and/or retrieved. I therefore also respectfully submit that there is reasonable cause to permit the search of the SUBJECT

PERMISES to occur at any time in the day or night for the fourteen day period of time permitted in the Warrant.

**CONCLUSION**

7. I submit that this affidavit supports probable cause for a supplemental warrant to continue the search of the SUBJECT PREMISES, after 10:00 p.m. and continuing at any time of the day or night until complete.

Respectfully submitted,

Mosi K. Forde
Special Agent
U.S. Department of Health and Human Services, Office of Inspector General

Subscribed and sworn to before me
on **March 1, 2016:**

ROBERT C. MITCHELL
UNITED STATES MAGISTRATE JUDGE
**Pittsburgh, PA**

# ATTACHMENT A

*Property to Be Searched*

The property to be searched, that is, the SUBJECT PREMISES are the offices of Tiversa, located on the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, PA 15222, the address depicted in the photographs below. That address is a seven-story building. The numbers "606" can be seen at the entrance to the building. Tiversa owns the office building but only operates out of the aforementioned 2nd, 5th, 6th, and 7th floors.

The lobby of the building is located on the 1st floor with a security guard stationed at a desk. Two other businesses lease space on the 1st floor: HealthQuest Chiropratic and Joseph Orlando (a men's clothing store). The 3rd floor is vacant. The entire 4th floor is leased by Celli-Flynn Brennan Architects & Planners. The space leased by businesses other than Tiversa is not considered part of the SUBJECT PREMISES to be searched.


Butcher and The Rye
CVS Pharmacy
Ulrich Shoe Repair
Liberty Ave
Liberty Ave
Liberty Ave
Market St
PNC Legacy Project
606 Liberty Ave
Habitat
Triangle Park
Fifth Ave
Fifth Ave
Sign in
Radio Hybrid
Starbucks
The PNC Financial Services Group, Inc
Reed Smith LLP
Moneygram (inside
Google
Map

## ATTACHMENT B

***Items to Be Seized***

1. The items to be seized or imaged are evidence, information relating to, fruits, contraband, or instrumentalities of violations of 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements), as described in the affidavit, including but not limited to the following:

a. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

   i. any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa, including but not limited to: LabMD, Transportation Security Administration (TSA), Qualcomm, Renaissance Healthcare (or "Baylor"), Boies Schiller & Flexner, Capitol One, MetLife, Open Door Clinic, Wagner Resource Group, and/or American Express;

   ii. any statements or representations made or intended to be made, or records or information produced or intended to be produced, to any government entity concerning Tiversa or Tiversa's work and business practices, including but not limited to any communication with and/or investigation by the Federal Trade Commission or the U.S. House of Representatives Committee of Oversight and Government Reform; and

   iii. any records, documents, and information of any kind reflecting the identities of any coconspirators, accomplices, or aiders and abettors in the commission of the above offenses.

b. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to communications involving any Tiversa employee, officer, director, or agent (including but not limited to email, voicemail, instant messages, Skype chats, and any and all proprietary/internal electronic communication used by Tiversa, such as Spark) where the subject matter of those communications relates to Tiversa's business, including but not limited to

i. Any and all communications that refer or relate to the availability of any client or prospective client's records on any peer-to-peer network;

ii. Any and all communications that refer or relate to Tiversa's discovery of any client or prospective client's records on any peer-to-peer network;

iii. Any and all communications that refer to relate to Tiversa's marketing of its services to any client or prospective client, including but not limited to communications with such client or prospective client or third parties affiliated with clients or prospective clients (such as individuals whose personal identifying information Tiversa purported to have seen made available by a client or prospective client);

iv. Any and all communications that refer to relate to media and/or news coverage of data security breaches in general or Tiversa's services in particular; and

v. Any and all communications that refer or relate to Tiversa's business interest in clients or prospective clients retaining Tiversa's services.

c. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

i. Tiversa's accounting software including but not limited to Peachtree, Sage Software, and/or QuickBooks;

ii. Tiversa's proprietary systems/applications or systems/applications used by Tiversa including but not limited to File Renamer, Eagle Vision, Coveo (or Covio), Ayinger, RAD Importer, FAST, FileDetector, and the Dynamic Signature Profile;

iii. Tiversa's backend databases (e.g., Microsoft Access or SQL/SQLite);

iv. internal/"in-house" Tiversa work products including but not limited to tickets, monthly reports, P2P monitoring status reports, investigation response reports, breach protection reports, Year in Review reports, takedown notices, forensic/forensic investigation reports, and Incident Response Case (or "IRC") reports; and

v. any records in Tiversa's Data Store that refer or relate to any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa.

2. Any and all computers, electronic storage media, or digital devices used in the commission of the above-referenced offenses.

3. All records and logs that refer or relate to the HID Card Reader system installed and housed at SUBJECT PREMISES.

4. All records, documents, programs, applications, and materials that refer or relate to banks and financial institutions, including but not limited to bank statements, passbooks, deposit or withdrawal slips, canceled checks, bank receipts, bank checks, money orders, loan documents, mortgages, safe deposit box keys, credit card records, charge receipts, investment account records and retirement records showing any transfers and/or deposits connected to the offenses outlined above.

5. For any electronic storage media or digital device whose seizure is otherwise authorized by this warrant, and any electronic storage media or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software (and evidence of the lack of such malicious software), as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;

d. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. evidence of the times the COMPUTER was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

l. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

# Exhibit 1

AO 93 (Rev. 12/09) Search and Seizure Warrant

# UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

| | | |
|---|---|---|
| In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* | ) | |
| The Offices of Tiversa, located at 606 Liberty Avenue, Pittsburgh, PA 15222 | ) | Case No. [UNDER SEAL] 16-0180M |

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:
See Attachment A incorporated herein by this reference.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B incorporated herein by this reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before 14 days *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty United States Magistrate Judge *(name)*.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Jul 29, 2016 11:50 — Robert C. Mitchell
*Judge's signature*

City and state: Pittsburgh, Pennsylvania — Robert C. Mitchell, United States Magistrate Judge
*Printed name and title*

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

**Return**

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
*Executing officer's signature*

_____
*Printed name and title*

# ATTACHMENT A

*Property to Be Searched*

The property to be searched, that is, the SUBJECT PREMISES are the offices of Tiversa, located on the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, PA 15222, the address depicted in the photographs below. That address is a seven-story building. The numbers "606" can be seen at the entrance to the building. Tiversa owns the office building but only operates out of the aforementioned 2nd, 5th, 6th, and 7th floors.

The lobby of the building is located on the 1st floor with a security guard stationed at a desk. Two other businesses lease space on the 1st floor: HealthQuest Chiropratic and Joseph Orlando (a men's clothing store). The 3rd floor is vacant. The entire 4th floor is leased by Celli-Flynn Brennan Architects & Planners. The space leased by businesses other than Tiversa is not considered part of the SUBJECT PREMISES to be searched.


Butcher and The Rye
CVS Pharmacy
Ulrich Shoe Repair
Liberty Ave
PNC Legacy Project
606 Liberty Ave
Habitat
Triangle Park
Radio Hybrid
Starbucks
Sign in
The PNC Financial Services Group, Inc
Reed Smith LLP
Google
Map

# ATTACHMENT B

***Items to Be Seized***

1. The items to be seized or imaged are evidence, information relating to, fruits, contraband, or instrumentalities of violations of 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements), as described in the affidavit, including but not limited to the following:

a. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

i. any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa, including but not limited to: LabMD, Transportation Security Administration (TSA), Qualcomm, Renaissance Healthcare (or "Baylor"), Boies Schiller & Flexner, Capitol One, MetLife, Open Door Clinic, Wagner Resource Group, and/or American Express;

ii. any statements or representations made or intended to be made, or records or information produced or intended to be produced, to any government entity concerning Tiversa or Tiversa's work and business practices, including but not limited to any communication with and/or investigation by the Federal Trade Commission or the U.S. House of Representatives, Committee of Oversight and Government Reform; and

iii. any records, documents, and information of any kind reflecting the identities of any coconspirators, accomplices, or aiders and abettors in the commission of the above offenses.

b. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to communications involving any Tiversa employee, officer, director, or agent (including but not limited to email, voicemail, instant messages, Skype chats, and any and all proprietary/internal electronic communication used by Tiversa, such as Spark) where the subject matter of those communications relates to Tiversa's business, including but not limited to

i. Any and all communications that refer or relate to the availability of any client or prospective client's records on any peer-to-peer network;

ii. Any and all communications that refer or relate to Tiversa's discovery of any client or prospective client's records on any peer-to-peer network;

iii. Any and all communications that refer to relate to Tiversa's marketing of its services to any client or prospective client, including but not limited to communications with such client or prospective client or third parties affiliated with clients or prospective clients (such as individuals whose personal identifying information Tiversa purported to have seen made available by a client or prospective client);

iv. Any and all communications that refer to relate to media and/or news coverage of data security breaches in general or Tiversa's services in particular; and

v. Any and all communications that refer or relate to Tiversa's business interest in clients or prospective clients retaining Tiversa's services.

c. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

i. Tiversa's accounting software including but not limited to Peachtree, Sage Software, and/or QuickBooks;

ii. Tiversa's proprietary systems/applications or systems/applications used by Tiversa including but not limited to File Renamer, Eagle Vision, Coveo (or Covio), Ayinger, RAD Importer, FAST, FileDetector, and the Dynamic Signature Profile;

iii. Tiversa's backend databases (e.g., Microsoft Access or SQL/SQLite);

iv. internal/"in-house" Tiversa work products including but not limited to tickets, monthly reports, P2P monitoring status reports, investigation response reports, breach protection reports, Year in Review reports, takedown notices, forensic/forensic investigation reports, and Incident Response Case (or "IRC") reports; and

v. any records in Tiversa's Data Store that refer or relate to any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa.

2. Any and all computers, electronic storage media, or digital devices used in the commission of the above-referenced offenses.

3. All records and logs that refer or relate to the HID Card Reader system installed and housed at SUBJECT PREMISES.

4. All records, documents, programs, applications, and materials that refer or relate to banks and financial institutions, including but not limited to bank statements, passbooks, deposit or withdrawal slips, canceled checks, bank receipts, bank checks, money orders, loan documents, mortgages, safe deposit box keys, credit card records, charge receipts, investment account records and retirement records showing any transfers and/or deposits connected to the offenses outlined above.

5. For any electronic storage media or digital device whose seizure is otherwise authorized by this warrant, and any electronic storage media or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software (and evidence of the lack of such malicious software), as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;

d. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. evidence of the times the COMPUTER was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

l. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

# Exhibit 2

**UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| **IN THE MATTER OF THE SEARCH OF:**<br><br>**The Offices of Tiversa, located at 606 Liberty Avenue, Pittsburgh, PA 15222** | **UNDER SEAL**<br><br>**Mag. No.** 16-0180M |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Mosi Forde, a Special Agent for the United States Department of Health and Human Services ("HHS"), Office of Inspector General ("OIG"), Office of Investigations ("OI"), Digital Investigations Branch ("DIB"), Computer Crimes Unit ("CCU"), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, Pennsylvania (hereinafter, the "SUBJECT PREMISES"), as further described in Attachment A, for the items described in Attachment B, that is, evidence, information relating to, contraband, fruits, or instrumentalities of the following criminal violations: 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of

Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements).

2. I have been a Special Agent with HHS/OIG since February 2015. I am currently assigned as a Special Agent within HHS/OIG/OI/DIB/CCU where I investigate violations of United States laws. I am a graduate of the U.S. Department of Homeland Security, Federal Law Enforcement Training Center ("FLETC"), Criminal Investigative Training Program, and the HHS/OIG Special Agent Basic Training Program. As a Special Agent, I have conducted investigations into violations of federal law.

3. I have received specialized law enforcement training in advanced computer forensics techniques at FLETC, in Glynco, Georgia, where I obtained my Seized Computer Evidence Recovery ("SCERS") certification. From February 2011 until being appointed as a Special Agent, I was a Forensic Computer Examiner ("FCE") for HHS/OIG/OI/DIB, Digital Investigations Unit (DIU). I have personally provided search warrant support and forensic analysis on over 20 cases involving Medicare, Medicaid, Computer Crimes, Child Exploitation, and other matters. As a FCE, I have also obtained several advanced computer forensic accreditations such as the EnCase Certified Examiner certification. I am a graduate of the University of Maryland (College Park, Maryland) with a Bachelor of Arts degree in Criminology and Criminal Justice. I have also taught courses to newly hired Special Agents in computer techniques at the HHS/OIG, Special Agent Basic Training Program.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses while investigating this matter. This affidavit is intended to show there is sufficient probable cause for the requested

warrant and does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit there is probable cause to believe that violations of 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements) have been committed by Tiversa Holding Corporation, and subsidiaries, affiliates, branches, divisions, units, or offices of such company, including, but not limited to: Tiversa Incorporated, Tiversa IP, Tiversa Entertainment Group, Tiversa Labs, Tiversa Media, Tiversa Government Incorporated, Tiversa Media Incorporated, Tiversa Real Estate Holdings LLC, as well as officers, agents, and employees thereof (hereinafter collectively referred to as, "Tiversa"). I further respectfully submit there is also probable cause to search the SUBJECT PREMISES, described in Attachment A, hereby incorporated by reference, for evidence, instrumentalities, contraband and fruits of these crimes further described in Attachment B, also hereby incorporated by reference.

**PREMISES TO BE SEARCHED**

6. The SUBJECT PREMISES on the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, Pennsylvania, 15222, is the primary place of operation for Tiversa. I know this based on available database checks, including, but not limited, to the Manta Media database. Additionally, after conducting interviews of former and current Tiversa employees, I know the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, Pennsylvania, 15222, to be the

current location of Tiversa, and its network servers. Lastly, a recent surveillance operation confirmed the "606 Liberty Avenue" address as Tiversa's place of operations.

## PROBABLE CAUSE

## GENERAL BACKGROUND

7. On May 19, 2015, HHS/OIG/OI/DIB/CCU received a referral from the Federal Bureau of Investigation ("FBI") Northern Virginia Cyber Task Force and the United States Attorney's Office for the District of Columbia, regarding potential criminal offenses committed by TIVERSA, a Pittsburgh-based internet and data security company. This case is a joint investigation by HHS and the FBI.[1]

8. Among other things, the evidence set forth below demonstrates that (a) Tiversa used proprietary software to scan network traffic for peer-to-peer (also called "P2P") programs[2] and thereby identified data security vulnerabilities (*e.g.*, files exposed to other users on the internet) and acquired copies of proprietary, regulatory, and/or sensitive documents, including

---

[1] In addition, allegations regarding Tiversa were raised in other proceedings, including an administrative complaint proceeding before the Federal Trade Commission ("FTC"), which culminated in the issuance of an Initial Decision on or about November 13, 2015, by an FTC Chief Administrative Law Judge. The Initial Decision in *In the Matter of LabMD Inc.*, FTC Docket No. 9357, is available at https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf . Although the Initial Decision related to various claims that a specific respondent, LabMD, Inc. ("LabMD"), had failed to provide reasonable and appropriate security for personal information maintained on LabMD's computer networks, the proceedings involved evidence about Tiversa and its business practices, including evidence from Confidential Witness #1, as described below.

[2] As set forth in greater detail below, "peer-to-peer" or "P2P" file sharing permits Internet users, through the use of special software (of which Gnutella, LimeWire, and Kazaa, are examples), to search for and obtain and/or download files from the computers of other users on the network, and to make one's own files available to other users of the network.

documents containing personal identification information and protected health information; (b) Tiversa offered companies data and internet security services in relation to such files, including monitoring and/or data breach remediation services; and (c) Tiversa engaged in a fraudulent scheme which included the making of various false and fraudulent statements, pretenses, and representations to such companies in order to induce such companies to hire Tiversa, to retain Tiversa for ongoing services, and/or to expand their use of Tiversa's services. As set forth in greater detail below, such false and fraudulent statements, pretenses, and representations included false and fraudulent representations of the Internet Protocol addresses ("IP addresses") at which Tiversa purportedly located a company's sensitive documents, and false and fraudulent representations to companies that such sensitive documents had "spread" or "proliferated" to one or more other locations on the Internet, all for the purpose of inducing these companies to retain, maintain, or expand their use of Tiversa's monitoring or remediation services.

## BACKGROUND – INDIVIDUALS

9. Tiversa was founded by Robert James Boback (hereinafter "Boback") and Sam Hopkins in 2003. Boback currently serves as the President and Chief Executive Officer for Tiversa. Boback is also on the Board of Directors for Tiversa.

10. Confidential Witness # 1 (hereinafter "CW1") is a former Tiversa employee who worked as an analyst and Director of Special Projects at Tiversa from July 2007 to February 2014. According to CW1, in the course of his work at Tiversa, CW1 was granted access to Tiversa's internal network (*i.e.*, database servers, file servers, application servers, etc.) and other information technology ("IT") resources. CW1 could also remotely access such resources through a laptop.

CW1 stated that he often made digital copies of Tiversa's databases (including one called the "Data Store") to complete certain tasks and projects. CW1 maintained these copies on CW1's laptop and external hard drives. CW1 voluntarily provided copies of this digital media to criminal investigators.[3]

11. CW1 is a defendant in a pending civil action brought by Tiversa and Boback, in which Tiversa alleges against CW1 counts of tortious interference with contractual relations, civil conspiracy, and breach of contract. CW1 also has a contractual entitlement to a portion of any recovery of a relator's share in a pending *qui tam* civil matter under seal against Tiversa and Boback. These civil matters relate to the criminal conduct presently under investigation.

12. CW1 also has the following convictions, all misdemeanors or summary matters, and all guilty pleas: (1) DUI 1st Offense, 6/19/14; (2) DUI 2nd offense, 2/9/15; (3) DUI 3rd offense, 2/9/15; (4) Disorderly Conduct (Engaged in fighting), 4/22/14; (5) Disorderly Conduct, 8/12/14; (6) Harassment, 12/09/14; and (7) Driving without a license, 12/09/14. CW1 is on probation until August 9, 2020.

13. Confidential Witness # 2 (hereinafter "CW2") is a [redacted] Tiversa employee [redacted]

14. Confidential Witness # 3 (hereinafter "CW3") is a [redacted] Tiversa employee [redacted]

[3] CW1 received an order, requested by the U.S. Department of Justice, granting him immunity pursuant to 18 U.S.C. § 6004, dated November 14, 2014, after which CW1 testified in an administrative proceeding,

15. Confidential Witness # 4 (hereinafter "CW4") was the sole owner, President, and Chief Executive Officer of LabMD. LabMD was a privately held Georgia corporation, incorporated by CW4 in 1996. LabMD went out of business in about January 2014.

16. CW4 is the relator in the pending *qui tam* civil matter under seal in New York referenced in paragraph 11. LabMD is a defendant in an FTC action captioned *In the Matter of LabMD, Inc.*, FTC docket number 9357. After an evidentiary proceeding, the Administrative Law Judge issued an order dismissing the action, and it is currently on appeal to the Commission. CW4 and LabMD are two of the defendants in the pending civil action in Pennsylvania referenced in paragraph 11 in which Tiversa alleges against CW4 and LabMD counts of defamation, slander, commercial disparagement/trade libel; tortious interference with contractual relations; and civil conspiracy. These allegations were originally filed against CW4 and LabMD in the Western District of Pennsylvania, but they were later dismissed and re-filed in state court with the addition of defendants CW1 and Cause of Action. LabMD is the plaintiff in an action against Tiversa in the Western District of Pennsylvania, alleging conversion; defamation; tortious interference with business relationships; fraud; negligent misrepresentation; civil conspiracy; and RICO violations.

17. CW4 and LabMD are plaintiffs in a *Bivens* action against various individuals in the District of the District of Columbia. LabMD was a plaintiff in a 2011 action against Tiversa et al. in Georgia. The case was removed to federal court (11-cv-4044 (ND Ga.)) and was dismissed. LabMD was a plaintiff in two related actions against the FTC in 2013 and 2014: *LabMD, Inc. v.*

---

referenced in footnote 1, and was interviewed by investigators.

*FTC and five named Commissioners*, 13-cv-01787 (D.D.C Nov. 14, 2013) alleged, inter alia, that the FTC abused its statutory authority and acted ultra vires, and it was voluntarily dismissed on Feb. 19, 2014; *LabMD, Inc., v. FTC*, 14-cv-00810 (ND Ga. Mar. 20, 2014) made similar allegations and was dismissed for lack of jurisdiction.

**BACKGROUND – TIVERSA'S BUSINESS**

18. According to information provided by CW1 during various interviews with investigators, and sworn testimony by CW1 on May 5, 2015, before the FTC which I have read, Tiversa was a data security company that offered breach detection and remediation services. Tiversa used key word searches and automated search programs to search for sensitive information available primarily over a peer-to-peer network known as "Gnutella." A P2P network, described in somewhat more detail below, is a means of efficiently sharing information across the Internet with other users of the same P2P network. To be able to access a P2P network, a computer must have installed on it an application or client software that is designed to be able to interface and communicate with that P2P network. Such application or client software for the Gnutella P2P network includes applications known as "LimeWire," "Kazaa," and "BearShare."

19. According to CW1, Tiversa used a series of algorithms (that is, proprietary software), and other tools, to search P2P networks for documents of interest to its clients or potential clients, particularly data files containing sensitive information such as personal identifying information ("PII") or protected health information ("PHI"). Tiversa would download copies of the documents/data files that it found. Tiversa obtained such files either automatically using Eagle Vision, Tiversa's proprietary application, or as manual downloads by an individual employee, such as CW1. Tiversa's proprietary application would index the IP address from

which Tiversa downloaded any file from the P2P network and add, or "prepend," that IP address to the file name. Thus, once a file was downloaded by Eagle Vision, the originating/source IP address would automatically be prepended to the file name (*e.g.*, "[192.168.1.1]Healthcare_SSN.pdf"). However, CW1 stated that Tiversa could and did modify both the file name, including the prepended IP address, and the computer file directory, usually designated by IP address, where the file was stored, while CW1 was employed at Tiversa.

20. According to CW1, Tiversa maintained servers which stored data that Tiversa's searches downloaded from P2P networks, referred to as Tiversa's "data store" ("Data Store"). The Data Store contained both copies of files that Tiversa had downloaded from the P2P network, as well as information as to where the downloaded file had been located before download. According to CW1, data files were saved into Tiversa's Data Store in two ways. Tiversa's program, Eagle Vision, would automatically download files returned from Tiversa's searches and save the files in the Data Store in a folder identified by the IP address from which the files were acquired, or, alternatively, an analyst, such as CW1, would insert data into the Data Store folders that the analyst found using a stand-alone computer running a P2P client.

21. According to CW1, CW1's job included searching P2P networks using the standard P2P Gnutella clients, such as LimeWire or Kazaa, to supplement information that Tiversa's system may not have automatically identified and downloaded. For example, if Tiversa were looking for insurance information for a healthcare company, CW1 could search the Gnutella network using search terms, such as "insurance" or "report," seeking to identify exposed sensitive files. A file was "injected" (a phrase used by Boback and others at Tiversa) if it was downloaded manually, *i.e.*, using something other than the Eagle Vision application. After files were injected, they were

manually placed in Tiversa's Data Store. In addition to CW1, other Tiversa analysts would occasionally find files as well.

22. A company's sensitive data, like PII or PHI, could become accessible on a P2P network like Gnutella through a variety of ways. A corporate employee could, for example, install a P2P application on a corporate computer, thereby inadvertently exposing corporate files to the public, because the employee wanted to utilize the P2P network for personal purposes at work, like music sharing. Individuals could also remove sensitive or government classified files from authorized computers and load the files to personal or unauthorized computers that were connected to P2P networks.

23. According to CW1, Tiversa would attempt to monetize data files and potential data security breaches it identified either by selling a monitoring contract, pursuant to which Tiversa would search for certain key words for a period of time, or by selling a "one-off" service to remediate just the existing disclosure problem. According to CW1, a Tiversa monitoring services contract for a large financial company could cost as much as a million dollars per year, down to a few thousand dollars per month for monitoring contracts for small "mom and pop" companies.

**BACKGROUND – THE FRAUDULENT FILE MANIPULATION SCHEME**

24. According to CW1, Tiversa was having problems selling monitoring contracts and retaining clients. Consequently, Tiversa engaged in various fraudulent practices to attempt to induce companies whose information Tiversa had discovered and acquired to contract for Tiversa's services, or to maintain or expand existing contracts. For example, as set forth in greater detail below, an analyst at Tiversa would make it appear as though sensitive information that Tiversa had located on a company computer had "proliferated" or "spread" over the P2P network to computers

with different IP addresses, located in the United States and/or abroad, and then inform the company of the "spread" and emphasize the urgency of remediating it. "Spread" was a term or expression used by Tiversa to describe the proliferation of files or documents on P2P networks. In other words, if a file was spreading on the P2P network it meant that it was being downloaded and re-shared by multiple users. Tiversa would sometimes further falsely represent to a prospective client, or to a client whose business Tiversa was trying to keep, that one or more of the IP addresses to which sensitive data had spread was known to be associated with criminal activity, such as the IP address of a known identity thief. Such a misrepresentation could appear logical due to the expectation that identity thieves would be interested in, and trolling P2P networks in search of PII, PHI, and other sensitive data to steal.

25. To create "evidence" and substantiate allegations of data proliferation or spread across P2P networks, Tiversa, including CW1, would alter the information in its Data Store to reflect the false proliferation. Tiversa would substitute prepended IP addresses in file titles and move the files to different folders in a subdirectory of the Data Store associated with the IP addresses to which the files were supposed to have spread. This would suggest, falsely, that the files had been located and acquired by Tiversa's Eagle Vision program, or by a Tiversa analyst, at those additional IP addresses and then stored in the folders identified or associated with those IP addresses. Tiversa could then use this Data Store "evidence" to try to induce the company to purchase (or maintain) Tiversa's remediation services. According to CW1, the vast majority of files acquired by Tiversa were manipulated to fraudulently reflect spread. According to CW1, CW1 personally manipulated files to change information about IP address source location and to remove or alter metadata such as author information, and dates created and saved. CW1 also

stated that Boback discussed with CW1 how to modify files and create the false and fraudulent impression of file-spread, and instructed CW1 to do so for existing and prospective clients.

26. CW1 stated that it was Tiversa's normal business practice to conduct "cold calls" to entities whose sensitive files or information Tiversa had discovered on a P2P network. According to CW1, if the document contained highly sensitive information, Boback would oftentimes contact the entity himself. The purpose of these calls was to inform the entity of the data "leak," and, more importantly, to offer Tiversa's remediation and monitoring services. CW1 stated that Tiversa's analysts and sale representatives were told by Boback never to provide the entity with the IP address or geo-location of where the file was found. If the entity expressed doubt about Tiversa's claim to be in possession of the file, Tiversa would send, usually by email, a copy of the document as proof. If an entity agreed to hire Tiversa, a "Ticket" would be emailed to the entity.

27. According to CW1, Tiversa used "Tickets," otherwise known as "Incident Record Forms," formally to alert clients that sensitive files (*e.g.*, classified secrets, proprietary/regulatory documents, SSN's, DOB's, or other types of PII/PHI) had been discovered on a P2P network. According to CW1, these Tickets did not always coincide with or accurately state when Tiversa had actually discovered the file; CW1 stated that Boback would often instruct analysts to retain files to be used in future Tickets, and such future Tickets would usually indicate discovery of the files near the time of the sending of the Ticket. The purpose of this was falsely to imply that the discovery was recent and that any remediation efforts would therefore likely be effective. Tickets were usually three pages in length. The first page contained basic customer/client information, the name of the file discovered, and the IP address where it was found, as well as a

brief write-up that detailed more information about the file and the location it was found. If a client required more information about the disclosed file, the second page of the Ticket could be used by the client to request additional "P2P File Sharing Forensic Investigation Services" from Tiversa. The last page, called the "Investigation Request Form," listed the available "Forensic Services" offered by Tiversa. These services included "Disclosure Source Identification," "Identify Additional Disclosure Source Files," and "Proliferation Point Identification."

28. If a client desired more information about the disclosure, or if Tiversa wanted to communicate to a client a fraudulent allegation that a client's files had "spread" on the P2P network to promote more business, Tiversa would either generate a Forensic Investigation Report or Investigative Response Case ("IRC") Report. Depending on the forensic services requested in the previously issued Ticket, and Tiversa's motive in sending the Report, the Forensic Investigation Report would detail such information as the IP Geo-Location(s), the Internet Service Provider(s), and a more detailed description of the alleged source(s) of disclosure. IRC Reports were usually more detailed and contained such as information as a (usually false) file spread analysis and suggested actions to address the data leak. CW1 stated that the information found in these documents often contained manipulated (that is, false and fraudulent) file information such as the source IP addresses, the IP addresses listed as being disclosure sources, and file timestamp(s).

29. According to CW1, prior to sending a file to a client or prospective client, Tiversa would scrub a file of all its metadata (*e.g.*, author/ownership information) and would use a "file renamer" program to change file properties, such as file names and timestamps (*e.g.*, date created/modified). Tiversa would modify timestamps to corroborate Tiversa's account of when

files were discovered. Tiversa would then send a "clean" file – with the falsified and fraudulent metadata and file properties – to the client or prospective client as proof that the file was available on P2P network. Time stamps were changed, in part, to make it appear that the file had only recently been made available on the P2P network, or only recently spread, thereby implying a window of opportunity to remediate the problem.

30. According to an email obtained and reviewed by investigators, a Tiversa employee, on or about October 1, 2007, emailed a link to other Tiversa employees about a software application called "File Renamer Basic," stating that he had "found a really cool free tool . . . called File Renamer Basic. It allows you to make all kinds of changes to multiple file titles at a time. The best use for us will be prefixing IP addresses to files that [CW1] and I find on the Limewire lab. I was able to prefix an IP address to 306 files that [CW1] found, in about 60 seconds. I can show you how to use it when I return." In January 2016, CW3 told investigators that the file renamer program is most likely still installed on a number of Tiversa analysts' computers.

31. According to CW1, while he worked at Tiversa, CW1 compiled a list of approximately 12-15 "burnt," meaning inactive, IP addresses. The terms "Burnt IP addresses" or "burnt IPs" were used by CW1 and others at Tiversa to describe IP addresses that had been used by individuals in the commission of crimes, such as trafficking in child pornography[4] or identity theft, but which became known to law enforcement and thereafter were no longer active. CW1

---

[4] According to CW1, in the past, CW1 independently assisted law enforcement to identify P2P users sharing child pornography. As a result of this law enforcement relationship, CW1 would sometimes learn of the arrest/detainment of these individuals. Once CW1 knew these users were no longer "active" he would add their IP addresses to his list of "burnt IPs."

and Tiversa used these burnt IPs, which included foreign IP addresses, in making false claims to clients and prospective clients respecting the source from which Tiversa had acquired information or the location to which information had spread on P2P networks. Such "spread" would often be communicated to companies in emails containing "spread analysis reports."

32. According to CW1, the burnt IP address that CW1 and other Tiversa employees used most frequently to fraudulently convey spread was an IP address that originated from Apache Junction, Arizona. At the time, the Apache Junction IP address belonged to a known identify thief, sometimes referred to as an "information concentrator." According to CW1, the Apache Junction IP address was used for the majority of Tiversa's fraudulent Forensic Investigation Reports and IRC Reports as recently as 2014. Another burnt IP address frequently used by Tiversa belonged to an information concentrator in San Diego, California. Tiversa used such IP addresses associated with "information concentrators" because it was more plausible to prospective clients that their data could be found at IP addresses associated with identity thieves.

33. According to CW1, CW1 and Boback created an online persona known as, "Glen Breakwater" (hereinafter "Breakwater"), including through gmail and facebook accounts to which both CW1 and Boback had access. Boback and CW1 used Breakwater to serve as an "intermediary" between Boback and the media. CW1 stated that CW1 would normally sign into the account and Boback would "do the writing." Boback would use the Breakwater account to "anonymously" alert the media to data breaches or leaks affecting notable companies, mostly companies Tiversa had an interest in pursuing. CW1 stated that Boback would often deploy this tactic to increase the pressure on prospective (and sometimes current) clients to sign up for Tiversa data security monitoring/breach remediation services. For example, according to CW1, the

Breakwater account was used to contact the Washington Post to inform the media of a data breach at a DC area financial investment firm as further described below.

**BACKGROUND -- BOBACK'S INVOLVEMENT**

34. According to CW1, Boback was fully aware of and actively encouraged the process of file manipulation, including alterations to downloaded document metadata and the fraudulent representations of spread. Boback and CW1 would sometimes discuss it with other Tiversa employees present. According to CW1, if the file originated from a large or high profile company, Boback would contact the client or prospective client himself. Boback would usually inform the prospective client that its data was actively being downloaded and/or shared on P2P networks, when in fact there was only one disclosure source. In other words, according to CW1, Boback would falsely and fraudulently represent that a file had "spread," using the file information manipulated by CW1, for example, when in fact no such spread had occurred.

35. According to CW1, Boback would get involved with clients when he felt that Tiversa's sales personnel could not get the job done, or when a prospective high profile client needed to be "convinced." To convince these clients, Boback would often directly email the company's senior leadership. If Boback wanted to apply more pressure to the company, he would email a member of the company's Board of Directors to inform the Board of the alleged spread of the file(s). Boback also asked CW1 to collect the IP addresses of online visitors to Tiversa's website for later use as potential fraudulent P2P disclosure destinations.

36. CW1 provided investigators digital media containing certain emails and other documents copied from Tiversa's servers. Included in this media was an e-mail dated June 24, 2008, from Boback to several other Tiversa employees, which responded to an earlier message

from a prospective client asking a Tiversa representative what services Tiversa could provide at what cost. Boback's e-mail stated, "This is awesome…..3K/mo gets your info spread across the P2P…..5K/mo gets our monitoring…which one does he want? :-)."

**BOBACK'S FALSE AND CONFLICTING TESTIMONY REGARDING THE 1718 FILE**

37. On November 21, 2013, Boback testified in a deposition related to the FTC proceedings described in footnote 1, above. Boback testified about a certain file, known as the "1718 File," which belonged to a company called LabMD located in Atlanta, Georgia, as more fully discussed below. The original source from which Tiversa acquired the 1718 File was a material issue in the FTC proceedings. Boback testified that Tiversa discovered and acquired the 1718 File from four (4) different P2P networked IP addresses, none of which was a Georgia IP address used by or associated with LabMD. Boback, in other words, testified that, by the time Tiversa discovered the 1718 File, it had already "spread" beyond LabMD's computers. Boback acknowledged during his testimony that an Atlanta IP had a positive "hash match" but denied that Tiversa had actually downloaded the 1718 File from the Atlanta, Georgia, IP address. However, Boback also testified, at first, that the Atlanta IP address "…is most likely the initial disclosing source," but then later testified that "…if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source."[5]

38. Boback's testimony was knowingly false. First, according to CW1, Boback knew the 1718 File had originally been acquired by Tiversa from a LabMD computer in Atlanta, Georgia, which origination is memorialized in Tickets sent by Tiversa in 2008. Indeed,

---

[5] A "disclosure source" in this context is the IP address associated with the P2P networked computer that a leaked file was originally stored on and from which the file had spread to other IP addresses.

according to CW1, CW1 downloaded the file only from an IP address associated with LabMD in Georgia and nowhere else. Second, in an email, dated three months prior to his November 21, 2013, testimony, Boback acknowledged as much, writing that the 1718 File was "found to be in Georgia, which after a Google search, is where we found LabMD's office to be located." CW1 stated to investigators, and testified on May 5, 2015, before a Federal Administrative Law Judge, that, shortly after Tiversa received a Criminal Investigative Demand (CID) from the FTC in 2013, he was instructed by Boback to use the burnt IP addresses of "information concentrators" in San Diego, California, and Apache Junction, Arizona, to show in Tiversa's records, falsely, that the 1718 File had spread beyond the actual LabMD disclosure source to four other IP addresses. These IP addresses were to be the locations from which Boback would falsely testify on November 21, 2013, that Tiversa had located and downloaded the 1718 File.

39. On June 7, 2014, Boback was again deposed in connection with the FTC proceedings, and his testimony during this deposition contradicted his earlier testimony on November 21, 2013. On June 7, 2014, Boback testified that the 1718 File was downloaded by Tiversa from a total of seven IP addresses, not four as he had previously testified, including originally from an IP address in Atlanta, Georgia. A Tiversa Forensic Investigation Report (Incident Number "LABMD0001"), dated June 4, 2014, lists an Atlanta IP address as the original source from which Tiversa acquired the 1718 File – the same Atlanta IP address Boback had denied Tiversa had acquired the 1718 File during his 2013 FTC testimony. [6]

---

[6] As part of his Initial Decision, the FTC Chief Administrative Law Judge found that Boback was "not a credible witness concerning LabMD, the 1718 File, or other [related] matters," adding that "[h]aving observed . . . Boback's June 7, 2014 video deposition . . . [,] Boback was evasive and lacked forthrightness in response to questioning." Initial Decision at ¶¶ 160, 166.

## TIVERSA CREATED MALWARE -- ICHABOD

40. While conducting this investigation I learned from CW1 that at one point malware was developed at Tiversa for the sole purpose of generating more business. The malware (codenamed "Ichabod") was to be used to make more documents available on the P2P networks, according to CW1. The malware had no graphical user interface and could be embedded into any file type. Once the malware was embedded, it would be sent to prospective clients. Once downloaded, the malware would run in the background while covertly indexing and capturing file information and properties from the user's computer. Next, it would wait for an internet connection to be established so that it could beacon out it's coordinates on the Gnutella network. Tiversa developers/analysts would then be able to see not only the computer, but all its files. Tiversa's development of Ichabod is most likely to have occurred in 2010 or 2011. CW1 stated that Ichabod was only used in a testing environment when he was at Tiversa. Boback, according to CW1, produced a fake letter bearing either the FBI or Defense Intelligence Agency crest or logo to convince Tiversa developers that the project was "above board" after initially being rebuffed by those developers.

## TIVERSA VICTIMS

### LABMD AND CIGNA

41. LabMD was a clinical testing laboratory located in Atlanta, Georgia. According to information provided to law enforcement by CW1, sworn testimony by CW1 on May 5, 2015, before a Federal Administrative Law Judge, and Tiversa documents I have reviewed, Tiversa downloaded an internal LabMD insurance aging report (hereinafter "1718 File") and approximately 18 other LabMD documents from a peer-to-peer network on or about February 25,

2008. Insurance aging reports are spreadsheets of insurance claims and payments. The 1718 File is a 1,718 page report that contains PII, PHI, and other sensitive information for some nine-thousand (9,000) patients. The computer file name for the insurance aging report is "insuranceagaing_6.05.071.pdf". CW1 stated that he was the first to discover the 1718 File and that he downloaded it on behalf of Tiversa. Furthermore, CW1 stated he only observed the file in one location and that location was in Atlanta, Georgia. The IP address from which the 1718 File was downloaded was 64.190.82.42, and this IP address was then associated with Cypress Communications in Atlanta, Georgia. This computer, with the IP address 64.190.82.42, was used by LabMD to store the 1718 File and other files related to LabMD's business.

42. On or about April 18, 2008, a Tiversa Ticket/Incident Record Form (ID# "CIG00081") was generated for CIGNA, a health services company and a paying client of Tiversa at the time. I obtained a copy of this document and have reviewed it. This ticket was three pages in length and had Tiversa's insignia at the top of the document. Section 1 was titled "Customer Information" and listed "CIGNA" as the Organization Name. In Section 2 of the Ticket the "Incident Information" describes the severity of the incident as "Urgent." In Section 3 of the Ticket the "Disclosure Information" listed the following IP Address, 64.190.82.42. In Section 4, the "Incident Summary" stated the following: "On 4/18/08, 1 file was detected being disclosed by what appears to be potential provider of services for CIGNA. The information appears to be a single Portable Document Format (PDF) file that contains sensitive data on over 8,300 patients. Some of the information includes: Patients Full Name, SSN, DOB, Insurance Policy Numbers, Patient Diagnostic Codes, and other information. Of the 8,342 patient records, at least 113 appear to be listed as insured by CIGNA. After reviewing the IP address resolution

results, meta-data and other files, Tiversa believes it is likely that LabMD near Atlanta, Georgia is the disclosing source." The April 18, 2008, detection date was a deliberate misrepresentation to suggest greater urgency and opportunity to remediate the spread. As discussed above, the 1718 File was actually acquired by Tiversa on February 25, 2008, according to CW1. Section 5 of the Ticket was titled, "Additional Questions That Tiversa Can Address." Section 5 stated, "More information can be gathered related to this disclosure by leveraging Tiversa's P2P File Sharing Forensic Investigation Services. If requested, please fill out the Investigation Request form located below and submit to your Account Manager." Section 5 and the Investigation Request form then listed various investigation services Tiversa offered its customers, including CIGNA. In addition to possibly generating business from CIGNA, this ticket would have had another likely consequence, namely, CIGNA's contacting LabMD to inquire about the alleged data disclosure.

43. According to CW4, from approximately May through July 2008, via telephone and email, Tiversa, and more particularly Boback, attempted to induce LabMD to engage Tiversa's security services, claiming that Tiversa had acquired the 1718 File from a peer-to-peer network, which was true, and that Tiversa had continued to see individuals downloading or attempting to download copies of the file, which was a deliberate falsehood. Some of Tiversa's communications to LabMD contained what could have been construed as veiled threats or coercive language. Thus, for example, on or about May 22, 2008, Boback sent an email, a copy of which I have obtained and reviewed, with the subject line "Tiversa/LabMD" to a LabMD employee. In the body of the email, Boback stated the following: "I hope this email finds you

doing well. We have continued to see people searching for the file in question[7] on the P2P network by searching precisely for the exact file name of the file in question. They may or may not have been successful in downloading the file however. Although, our system has also recorded that the file still exists on the network (as of last Friday) although we have not attempted to download another copy. The longer the file resides on the network, the more difficult the remediation tends to be. Considering the presence of SSNs in the file, this disclosure should be remediated ASAP." Despite Tiversa's repeated efforts, LabMD refused to engage the services of Tiversa.

44. On or about June 6, 2008, an email with the subject line "LabMD" was sent from Boback to a LabMD employee. I have obtained and reviewed a copy of this email. The body of the email stated as follows:

> I hope this email finds you doing well. I wanted to follow-up with you as I have not heard anything regarding the disclosure at LabMD. I am not sure if you caught the recent press about Walter Reed Army Medical Center having a disclosure of over 1000 patients SSNs etc. The story of the disclosure has been picked up by over 200 publications. Since then, we have seen the usual increase in search activity on the P2P [] in attempt to find this and other information of this type. Given this fact, we should move to remediation very quickly. If you have been able to locate the source of the disclosure internally, that would be helpful. The file, however, will most likely have been already taken by secondary disclosure points which will need to be found and remediated.

45. In another email from Boback to a LabMD employee, dated July 15, 2008, a copy of which I have obtained and reviewed, Boback stated that "We have continued to see individuals searching for and downloading copies of the [1718 file]." According to CW1, this was untrue and a deliberate falsehood. The email went on to state:

---

[7] "The file in question" refers to the 1718 File.

> 43 of 50 states have very strict laws requiring the immediate notification of the affected individuals. It is very important that you contact the individuals asap. I know this breach is troubling, however it is important to note that LabMD is not the only company that has been affected by this type of breach. This is widespread problem that affects tens of thousands of organizations and millions of individuals. I am not sure if you read the Washington Post, but there was an [sic] front page article last week involving a widely reported file sharing breach of Supreme Court Justice Stephen Breyer's SSN and personal data. Wagner Resources, the investment firm responsible, took immediate action to solve the problem which resonated with the affected individuals. In fact, many of the individuals whose information was disclosed contacted the owner of the firm to say that HE was the victim of this relatively unknown, although dangerous, security risk.

In fact, as described in greater detail below, it was Tiversa that obtained the referenced sensitive data from Wagner Resources and alerted the Washington Post to such. Tiversa notified Justice Breyer of the data leak before notifying Wagner Resources, just as Tiversa notified CIGNA before notifying LabMD, expecting Justice Breyer to contact Wagner Resources, according to CW1, as more fully discussed below.

46. On July 23, 2008, Boback sent an email to an attorney representing LabMD. I have obtained and reviewed a copy of this email. In the email, Boback stated to the attorney, "please confirm that you and/or your client (LabMD) are in compliance with state and federal breach notification laws regarding the disclosure of the estimated 9000 SSNs of the patients that have received services by LabMD."

47. Finally, on November 21, 2008, an attorney for LabMD memorialized a conversation he had had with an attorney for Tiversa. I have obtained and reviewed a copy of this memorandum. The Tiversa attorney indicated that he had been talking to the Federal Trade Commission because, according to Tiversa's attorney, "there are laws in place regarding leaks of personal information. [Tiversa] is concerned about being sued for having knowledge of the

breach and not reporting it/doing something required under the law." Tiversa's attorney then encouraged further communication to discuss the matter.

48. On or about May 13, 2008, at approximately 11:12AM, CW1 sent an email with the subject line "LabMD" to Boback. This email included an attachment with the filename "LabMD.zip." Minutes later, at approximately 11:25AM, Boback forwarded that email, with the subject title "FW: LabMD," to a LabMD employee. I have obtained and reviewed a copy of this email. In the body of the email, Boback stated "Per our conversation, please review the attached file to confirm its accuracy. I will have the engineer review to see when our systems first detected/downloaded the file from P2P network. At this point, I do not have that information but I will forward it as soon as I get it." According to CW4, the encrypted attachment contained a partial copy of the 1718 File. No other file(s) were included. Upon reviewing this document, CW4 stated that he immediately knew where the document originated. CW4 stated that the 1718 File, like other insurance aging reports, are distinct because they are created using an application known as Lytec, which was primarily used by LabMD's billing department. Moreover, the dissemination of these insurance aging reports was the responsibility of LabMD's billing manager. CW4 stated that LabMD's billing department consisted of approximately six to eight workstations.

49. As part of LabMD's internal investigation, CW4 stated that LabMD quickly identified the user and lone computer that contained the "LimeWire" P2P software application that had allowed Tiversa to download the 1718 File, and deleted the application from that computer. Removal of the LimeWire application from the billing manager's computer was completed by the afternoon of May 13, 2008. Additional investigative steps were taken by

LabMD, such as searching other LabMD computers for file sharing software, and also conducting independent searches on P2P networks for the 1718 File. LimeWire, or any other file sharing software, were not found on any LabMD computer, other than the billing manager's. Searches on P2P networks for the 1718 File yielded no results. CW4 stated that the 1718 File should not have been available on P2P networks after May 13, 2008.

50. On or about August 8, 2008, an email with the subject line "LabMD File Spread" was sent from CW1 to another Tiversa employee. I have obtained and reviewed a copy of this email. The body of this email contained three unique IP addresses. The first IP address, 64.190.82.42, was listed as "Orig Source" with the date "4/18/08." That IP address, according to CW1, is the IP address from which Tiversa acquired the 1718 File, not on April 18, 2008, but February 25, 2008. The second IP address, 64.190.79.36, was listed as "IP Shift" with the date "8/1/08." An "IP shift" would likely refer to a computer or other device accessing LabMD's ISP, Cypress Communications. According to CW1, the 1718 File was never acquired from this IP address, or any other, besides what was referred to as the original source, 64.190.82.42. The third IP address, 68.8.250.203, was listed as "Info Concentrator" with the date "8/5/08." "Info Concentrator," according to CW1, was another expression for identity thief, and this IP address, located at that time in San Diego, California, was known to Tiversa to have been used at one point by an identity thief.

51. On or about August 12, 2008, another Tiversa Forensic Investigation Report was generated for CIGNA. I have obtained and reviewed a copy of this Report. In the Report's Introduction, it states the reason for the Report: "CIGNA asked Tiversa to perform Forensic Investigation activities related to [Ticket No. CIG00081, discussed above in paragraph 42] in

order to ascertain if any of the disclosed files have proliferated across the P2P." The report incorporated the misinformation contained in the August 8, 2008, email discussed above, to suggest to CIGNA, falsely, that the data disclosure first reported in the CIGNA Ticket generated on April 18, 2008, had grown more severe. The Forensic Investigation Report is five pages in length and has Tiversa's insignia at the top of the document. The date "August 12, 2008" is stamped at the bottom of the first page. Section 1 contains an "Introduction" and summarizes the original April 18, 2008, Ticket. Section 2.1 is titled "File Proliferation Analysis" and includes a three row chart, listing the original IP address where Tiversa first observed (and acquired) the 1718 File and two more IP addresses to which the 1718 File had allegedly "proliferated." According to CW1, no such "proliferation" ever occurred. The chart appears as follows:

| Proliferation Point | File Title | IP Address | Date Observed | IP Geo-Location | ISP | Source |
|---|---|---|---|---|---|---|
| 0 | insuranceaging_6.05.071.pdf | 64.190.82.42 | 4/18/08 | Atlanta, GA | Cypress Communications | Original Source from Ticket #81 |
| 1 | insuranceaging_6.05.071.pdf | 64.190.79.36 | 8/1/08 | Oakwood, GA | Cypress Communications | Probably an IP shift of original source |
| 2 | insuranceaging_6.05.071.pdf | 68.8.250.203 | 8/5/08 | San Diego, CA | Cox Communications | Unknown (based on other files observed, possible Information Concentrator) |

Beneath this chart, the Report explained:

> Based on other files available at the new IP addresses, Proliferation point number #1 [] is most likely an IP shift from the original disclosing source identified in Ticket #81. However, the other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator. Because Tiversa analysts were only able to visually observe these new sources, rather than actually download files, further data collection and analysis may be required for full source identification of the proliferation points.

In Section 3 of the Report, titled "Conclusion/Suggested Actions," the Report stated:

> It appears evidence that the files from Ticket #81 have proliferated across the P2P and are available from additional IP addresses. However, clear identification of these new sources is not conclusive at this time. Tiversa will update this report as new information becomes available. In the meantime, CIGNA and/or LabMD investigations of the data currently available could be executed. If additional data from Tiversa is required, it can be provided – for instance, a full listing of files disclosed from the original source (even if those files are not related to CIGNA) can be made available.

52. On or about September 5, 2013, an email with the subject line "Tiversa" was sent from Boback to two other Tiversa employees. I have obtained and reviewed a copy of this email. In the body of the email, Boback stated in part the following regarding the LabMD 1718 File: "In 2008 while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable."

53. As discussed above, on or about November 21, 2013, Boback was deposed in connection with FTC proceedings. During the deposition, Boback testified that the 1718 File was found at four (4) different IP addresses. These four new IP addresses are not identified or referenced in the Tiversa Ticket to CIGNA generated on or about April 18, 2008, the CIGNA Forensic Investigation Report generated on or about August 12, 2008, or the CW1 Email sent on or about August 8, 2008. Boback testified that the four IP addresses were 68.107.85.250, in San Diego; 173.16.83.112, in Apache Junction, Arizona; 201.194.118.82, in Costa Rica; and 90.215.200.56, in London, United Kingdom. This deposition introduces a new, and slightly varied, version of the San Diego IP address earlier referenced in the CIGNA Ticket, which was

68.8.250.203. During the deposition Boback testified on at least two occasions that Tiversa did not "download" the 1718 File from Atlanta, but stated that Atlanta was the "initial disclosing source." CW1 informed investigators, and testified on May 5, 2015, before a Federal Administrative Law Judge, that Boback had instructed CW1 to modify the 1718 File to make it appear that the file had been downloaded from the four foregoing IP addresses, and not from LabMD's server in Atlanta, Georgia, because Tiversa was in a dispute with LabMD. CW1 stated that the Apache Junction, Arizona, and the San Diego, California, IP addresses were at one time associated with known information concentrators. Additionally, CW1 stated that he was asked by Boback to lie at a deposition about the "spread" of the 1718 File, and that he was physically assaulted in a Tiversa elevator by Boback when he refused to comply.

54. [redacted]

55. On or about May 29, 2014, at approximately 2:40 PM, an email with the subject line "files" was sent from a Tiversa employee to Boback. This message contained no text in the body. The email included an attachment that contained the 19 LabMD files originally downloaded by Tiversa on February 25, 2008. All of the files had the Atlanta, Cypress Communications, IP address prepended to the file name. Of the 19 files, one file bears a nearly identical filename to the 1718 File; the file is titled "insuranceaging_6.05.071_track.pdf," whereas the original title of the

1718 File was "insuranceagaing_6.05.071.pdf." A copy of this email and its attachment were provided to investigators.

56. [redacted]

57. On or about June 4, 2014, a Tiversa Forensic Investigation Report was generated ostensibly for LabMD, although LabMD never accepted the services of Tiversa and ceased doing business in about January 2014. I have obtained and reviewed a copy of this Report. The Forensic Investigation Report was 16 pages in length and "Prepared for LabMD" is written under the title of the document on page 1. Section 2 of the Introduction to the Report is titled "Incident Information," and describes the severity of the incident as "Urgent." Section 3 of the Introduction, titled "Preliminary Disclosure Information," lists the IP Address 64.190.82.42.

Section 4 of the Introduction, titled "Incident Summary," states in part: "On 2/5/2008, Tiversa systems detected 1 file being disclosed on P2P file sharing networks. The detected file appears to be a 1,718 page 'Insurance Aging' Report relating to 'LABMD. Incorporated'." The Incident Summary went to state, "Upon further analysis, 19 total files were detected being disclosed from this IP address on various dates between 3/7/2007 and 2/25/2008." The Incident Summary concludes, "Upon reviewing the metadata and files emanating from this source, Tiversa believes the disclosure source may be an individual employed with LabMD."

58. Section 2.2 of the Forensic Investigation Report is titled, "File Spread analysis." The Section includes a seven row chart listing seven different IP addresses at which Tiversa claimed it had found LabMD files, including the 1718 File. The chart appeared as follows:

File Spread Analysis – IP Summary Table

| Source# | IP Address | Disclosure Date(s) | ISP | Geolocation** | Total Files |
|---|---|---|---|---|---|
| Source 1 | 64.190.82.42* | 3/7/2007 - 2/25/2008 | CYPRESS COMMUNICATIONS LLC | ATLANTA, GEORGIA, US | 19 |
| Source 2 | 68.107.85.250 | 2/5/2008 - 9/20/2011 | COX COMMUNICATIONS INC. | SAN DIEGO, CALIFORNIA, US | 3,302 |
| Source 3 | 173.16.83.112 | 11/5/2008 - 2/14/2009 | MEDIACOM COMMUNICATIONS CORP | CHICAGO, ILLINOIS, US | 1,832 |
| Source 4 | 201.194.118.82 | 4/7/2011 | SAN JOSE (SANJOSECA.GOV) | SAN JOSE, SAN JOSE, CR | 33 |
| Source 5 | 90.215.200.56 | 6/9/2011 | EASYNET LTD | LONDON, ENGLAND, UK | 47 |
| Source 6 | 71.59.18.187 | 5/5/2010 - 11/7/2012 | COMCAST CABLE COMMUNICATIONS HOLDINGS INC | ALPHARETTA, GEORGIA, US | 254 |
| Source 7 | 173.16.148.85 | 2/23/2009 - 11/7/2012 | MEDIACOM COMMUNICATIONS CORP | NASHVILLE, TENNESSEE, US | 520 |

Section 2.2 stated that all the IP addresses listed were detected to possess the 1718 File. According to CW1, the information in this Forensic Investigation Report is false. No LabMD

files, including the 1718 File, were found or downloaded by Tiversa from any IP address other than LabMD's own IP address, at Cypress Communications, in Atlanta, Georgia, which is listed as "Source 1" in the chart. Further, the files were discovered and downloaded at "Source 1" in February 2008, not at any time in 2007. The "spread" of the files represented in this Report was a deliberate misrepresentation by Tiversa.

59. As discussed above, on June 7, 2014, Boback testified at a deposition relating to a FTC action. In his testimony, Boback stated that the 1718 File and other LabMD files were discovered and downloaded by Tiversa from all seven sources identified in the June 4, 2014, Tiversa Forensic Investigation Report chart, copied above. This testimony was false, according to CW1. The files were recovered only from what Tiversa identified as "Source 1."

60. CW1 provided investigators two compact discs that contained, among other things, copies of portions of Tiversa's Data Stores. More specifically, one disc contained copies of the Data Store pertaining to files prepended with the IP address 68.107.85.250. This copy was made on or about October 6, 2008, by CW1. The second disc contained copies of the contents of the same Data Store IP folder, but the copy was made by CW1 on or about February 9, 2009. CW1 stated that these snap shots represented the content of the IP folder at the time they were copied. The IP address 68.107.85.250 was one of the IP addresses Tiversa claimed was associated with a known identity thief and where Tiversa claimed to have detected the 1718 File on February 5, 2008, according to the LabMD Forensic Investigation Report, discussed above. Yet, a global search of the discs by investigating agents for the 1718 File yielded no hits.

61. CW1 also made a copy of the Tiversa Data Store IP folder for IP address 173.16.83.112 on or around July 29, 2009, which CW1 provided to investigators on a hard drive.

This IP address, associated with Apache Junction, Arizona, and later Chicago, Illinois, was also one of the IP addresses Tiversa claimed was associated with a known identity thief, and where Tiversa claimed to have detected the 1718 File on November 5, 2008, according to the LabMD Forensic Investigation Report, discussed above. This folder contains 1,826 files, a figure similar to the "1,832" listed in the LabMD Forensic Investigation Report. Each file in this folder has the Chicago/Arizona IP address prepended to the filename. The last modified date of the files found in this directory range from "11/5/08 – 2/14/09," which corresponds exactly with the LabMD file "Disclosure Dates" in Tiversa's LabMD Forensic Investigation Report. A global search of the Chicago/Arizona IP folder for the 1718 File yielded no hits.

AMERICAN EXPRESS

62. On or around January 3, 2008, CW1 recalled working on two American Express (hereinafter "AMEX") Tickets while employed at Tiversa. One of these tickets involved encryption keys with a high end/luxury AMEX credit card, likely the Centurion Card. CW1 stated that he first identified the encryption keys on a P2P network computer. At the direction of Boback, CW1 prepended fictitious IP addresses to the file name of the document to give the appearance that the encryption keys spread to multiple countries and locations. CW1 stated that at least two of the fictitious IP addresses were foreign addresses, and another was possibly the Apache Junction, Arizona, IP address used in the LabMD incident. According to CW1, he and Boback were the only two at Tiversa who knew about this specific instance of adding fictitious IP addresses. The second AMEX Ticket involved a text file, containing a large collection of AMEX credit card numbers that Tiversa had found on a P2P network computer. CW1 stated that Boback instructed him to prepend a fictitious IP address, associated with a location in Mexico,

into the name of this file to give the false appearance the document had spread to an IP address abroad. CW1 believes the timeline of these two events likely occurred towards the end of the AMEX contract in order to show the value of Tiversa's services. CW1 recalls Boback telling him that Tiversa was struggling financially and that if Tiversa were to lose AMEX as a client, Tiversa could not afford payroll.

63. On or about January 4, 2016, a representative from American Express (hereinafter "AMEX EMP") was interviewed by a law enforcement agent participating in this investigation about AMEX's prior business relationship with Tiversa. AMEX EMP stated that Tiversa was hired at a time when AMEX was observing a growing number of AMEX employees who had installed P2P software on their computers. Once Tiversa was hired, Tiversa provided AMEX with Tickets (or Incident Record Forms), and later informed AMEX that its documents had "spread" on P2P networks. At or near the Tiversa contract end date, AMEX made the decision not to renew because they determined that the influx of P2P software installations had subsided.

64. AMEX EMP stated around the time the contract with Tiversa was about to end, AMEX was contacted by Tiversa and told that a document containing proprietary "encryption keys" was available on P2P networks and, according to Tiversa, had spread to other countries. Once AMEX was informed of this purported spread, AMEX had to re-issue credit cards to a specific international region. The estimated cost for the reissuance of the credit cards was at least $1 million dollars, according to AMEX EMP. AMEX EMP stated that they would not have done business with Tiversa had they known that the reports of AMEX documents having spread on P2P networks were fraudulent. AMP EMP did not recall precisely how much money was

directly paid to Tiversa by AMEX, but speculated that it was about "several hundred thousand dollars."

WAGNER RESOURCE GROUP

65. According to CW1, as well as Tiversa documents provided to law enforcement by CW1, from in or about February 2007 through in or about June 2007, Tiversa, through the application of its Eagle Vision automated search and download software, discovered and acquired documents on a P2P network relating to Wagner Resource Group (hereinafter "WRG"), a financial services firm located in McLean, Virginia. The president of WRG is Phylyp Wagner (hereinafter "Wagner"), whom I and other investigators have interviewed. The documents acquired by Tiversa were located on a WRG employee computer assigned IP address 70.183.6.112 in Fairfax, Virginia; this employee had installed a P2P application on his/her WRG computer unbeknownst to Wagner.

66. CW1, who joined Tiversa in about July 2007, discovered the downloaded WRG files in Tiversa's Data Store in 2008, prepended with the originating IP address of 70.183.6.112. Upon instructions from Boback, CW1 worked to create the false impression that the files acquired from WRG's employee computer had "spread" to assist in monetizing the files, and to persuade WRG that WRG needed Tiversa's services.

67. On or about June 22, 2008, CW1 sent an email to Boback and Chris Gormley, a former Tiversa employee. The body of CW1's email noted in part, "Attached is the file spread for the two files that we were working on Friday afternoon/evening." On or about the same day, the email was forwarded to Keith Tagliaferri, a current Tiversa employee and Griffin Schultz, a former Tiversa employee. I have obtained and reviewed a copy of the original and forwarded

email. The body of the forwarded email noted, "…fyi…". The forwarded email had an attachment named "File Spread – Wagner Files.doc." "File Spread" was listed at the top of this document and just below it was referenced a date, "6/22/08 @ 1645." This document listed two files, "SSN and DOBs.rtf" and "ACT SSN DOB.rtf." The document had a picture of a map, and, below the map, listed 19 unique IP addresses, followed by the city, state, and/or country. Some of the cities listed were Livingston, New Jersey; Washington, D.C.; Long Beach, California; Fairfax, Virginia; New Orleans, Louisiana; Tijuana, Mexico; Colombo, Sri Lanka; Reston, Virginia; and Santafe De Bogota, Columbia.

68. According to CW1, at the direction of Boback, CW1 falsely listed the IP addresses in the "file spread" document to give the appearance to Wagner that the documents were downloaded by individuals throughout the country and the world. According to CW1, in fact, the document was only downloaded by Tiversa from one IP address, that being the WRG IP address of 70.183.6.112 in Fairfax, Virginia. According to CW1, CW1 and Boback knew that the purpose of adding fictitious IP addresses was to generate additional revenue from WRG; but for the false appearance of the "file spread," there would have been little or no reason to hire Tiversa because WRG could have resolved the matter by simply removing the P2P application from that computer.

69. CW1 indicated that he tracked the false WRG file spread IP addresses in a spreadsheet. CW1 provided to investigators a hard drive containing multiple files, including files related to WRG. One of the files was named, "File Listing With Spread Analysis.xls." The document's properties list the author as the first initial and last name of CW1, and date of creation as June 24, 2008. This document listed 87 WRG files that had been located on the

WRG employee computer through the P2P network, and identified the documents that Tiversa had falsely claimed to have spread. This document listed 10 WRG files that had purportedly spread, including files named "ACT SSN DOB.rtf" and "SSN and DOBs.rtf." Under a worksheet named "Spread List," again 10 files, including "ACT SSN DOB.rtf" and "SSN and DOBs.rtf," had multiple IP addresses associated with the file names. File "ACT SSN DOB.rtf" had approximately 3 IP addresses and File "SSN and DOBs.rtf" had approximately 18 IP addresses. Each of the 10 files had the same IP address highlighted in yellow. This IP address was 70.183.6.112 in Fairfax, Virginia, which was the original and only true source of Tiversa's WRG download, as is also reflected in the document entitled "File Spread – Wagner Files.doc". All of the file listings in the "File Listing With Spread Analysis.xls" document indicate that the 10 documents falsely represented as having spread were acquired from the false IP addresses on or before June 21, 2008. The spread sheet appeared as follows:

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | IP Address | File # | File Title | Spread | Notes | Proliferation Points | IP 1 | Date Acquired |
| 2 | [70.183.6.112 | 2 | ACT SSN DOB.rtf | Yes | | 2 | 70.183.6.112 | 3/22/2007 4:33 |
| 3 | | | | | | | 172.190.128.150 | 4/11/2007 7:33 |
| 4 | | | | | | | 71.107.225.11 | 4/17/2007 1:54 |
| 5 | [70.183.6.112 | 7 | [redacted].pdf | Yes | | 1 | 70.183.6.112 | 3/16/2007 3:43 |
| 6 | | | | | | | 76.214.138.212 | 4/17/2007 1:08 |
| 7 | [70.183.6.112 | 9 | [redacted].doc | Yes | | 1 | 70.183.6.112 | 3/16/2007 0:53 |
| 8 | | | | | | | 74.96.215.26 | 4/18/2007 1:56 |
| 9 | [70.183.6.112 | 11 | [redacted].doc | Yes | | 1 | 70.183.6.112 | 2/5/2007 12:07 |
| 10 | | | | | | | 67.100.157.42 | 10/31/2006 2:49 |
| 11 | [70.183.6.112 | 39 | [redacted].doc | Yes | | 1 | 70.183.6.112 | 4/16/2007 12:57 |
| 12 | | | | | | | 71.146.206.125 | 6/7/2007 17:59 |
| 13 | [70.183.6.112 | 45 | [redacted].pdf | Yes | std file | 6 | 70.183.6.112 | 4/17/2007 13:29 |
| 14 | | | | | | | 70.82.184.29 | 4/19/2007 0:31 |
| 15 | | | | | | | 66.142.189.3 | 6/10/2007 4:56 |
| 16 | | | | | | | 68.94.76.91 | 6/16/2007 21:04 |
| 17 | | | | | | | 68.88.131.51 | 6/22/2007 15:45 |
| 18 | | | | | | | 66.138.73.43 | 6/25/2007 3:12 |
| 19 | | | | | | | 66.137.148.248 | 6/27/2007 0:51 |
| 20 | [70.183.6.112 | 64 | [redacted].doc | Yes | | 1 | 70.183.6.112 | 3/15/2007 19:33 |
| 21 | | | | | same source as file #7 | | 76.214.138.212 | 4/17/2007 0:58 |
| 22 | [70.183.6.112 | 71 | [redacted].pdf | Yes | same as file #39 | 1 | 70.183.6.112 | 5/30/2007 12:47 |
| 23 | | | | | | | 71.146.206.125 | 6/7/2007 17:29 |
| 24 | [70.183.6.112 | 80 | [redacted].pdf | Yes | std file | 2 | 70.183.6.112 | 4/15/2007 0:20 |
| 25 | | | | | | | 213.207.246.80 | 5/16/2007 13:39 |
| 26 | | | | | | | 213.207.246.80 | 5/16/2007 13:39 |
| 27 | [70.183.6.112 | 83 | SSN and DOBs.rtf | Yes | | 18 | 70.183.6.112 | 3/21/2007 19:43 |
| 28 | | | | | | | 75.213.54.124 | 3/21/2007 21:24 |
| 29 | | | | | | | 75.212.52.141 | 3/23/2007 7:33 |
| 30 | | | | | | | 75.213.111.97 | 3/24/2007 23:52 |
| 31 | | | | | | | 75.212.120.120 | 3/25/2007 16:11 |
| 32 | | | | | | | 75.212.109.115 | 3/27/2007 17:37 |
| 33 | | | | | | | 70.166.14.66 | 4/4/2007 7:53 |
| 34 | | | | | | | 75.213.149.56 | 4/4/2007 9:29 |
| 35 | | | | | | | 75.212.60.2 | 4/13/2007 16:36 |
| 36 | | | | | | | 201.170.49.149 | 4/14/2007 4:11 |
| 37 | | | | | | | 201.170.1.38 | 4/14/2007 18:22 |
| 38 | | | | | | | 71.107.225.11 | 4/17/2007 1:53 |
| 39 | | | | | | | 75.213.97.239 | 4/27/2007 21:21 |
| 40 | | | | | | | 75.213.108.98 | 4/28/2007 0:13 |
| 41 | | | | | | | 65.188.53.80 | 4/28/2007 6:12 |
| 42 | | | | | | | 201.170.6.45 | 4/28/2007 14:28 |
| 43 | | | | | | | 124.43.209.101 | 6/3/2008 14:57 |
| 44 | | | | | | | 200.62.61.124 | 6/21/2008 3:12 |

70. A document named "ACT SSN DOB.rtf" was located on the hard drive provided by CW1. The document properties indicate that it was last modified on or about June 24, 2008. It was approximately 154 pages and listed client names and the PII associated with those clients. According to the file, CW1, and Wagner, the PII and names were for clients of WRG.

71. A document named "Wagner IRC Report – V1.doc" was also located on the hard drive provided by CW1. The document properties listed the author as "Chris Gormley." The file appeared to be a draft of an Investigation Response Case Report intended for WRG. The file properties indicate that the last modified date was on or about July 22, 2008. The report listed 87 files which appear to be associated with WRG. The report also listed 10 files which had purportedly spread including the "ACT SSN DOB.rtf" and "SSN and DOBs.rtf" files.

72. According to CW1, Boback and CW1 each took several client names from the downloaded WRG documents and contacted clients to notify them their PII was available on the P2P network. CW1 specifically recalled Boback bragging about how he got a hold of a judge in Maryland. According to CW1, Wagner attempted to call Tiversa but Boback refused to take his calls until Boback and CW1 had spoken to enough clients. There were two reasons for this, according to CW1. The first was that Boback wanted the clients – and particularly high profile clients – to contact WRG to inquire about the file leak to pressure Wagner to remediate the problem.[8] The second was that, once a business services/breach detection and remediation contract was signed between Tiversa and WRG, Tiversa signed a non-disclosure agreement which would prevent them from calling WRG's clients.

---

[8] The same pattern was observed, above, respecting LabMD when Tiversa contacted CIGNA before contacting LabMD expecting CIGNA to contact LabMD.

73. [redacted], Boback called one of WRG's clients and claimed that a sensitive document belonging to WRG was available on the internet. About a week later, an article in the Washington Post was written on the WRG data leak. Wagner verified that the document Tiversa found was the property of WRG.

74. [redacted], Boback told him that WRG's documents were located in multiple locations throughout the world. Wagner therefore had a sense of urgency to resolve this matter quickly because of the alleged spread. Wagner specifically recalled asking Boback why his documents were located in Asia; Boback replied that Asia was where criminals manufacture credit cards.

75. On or about June 23, 2008, Wagner signed a contract with Tiversa to address the leaked documents. The contract was countersigned by Boback and was faxed on or about the same day. A fax cover sheet indicated the sender was Griffin Schultz.

76. [redacted] These documents included a folder named "Ticket_WAGNER0001." Numerous sub-folders were located within this folder. One of the files identified was a Word file named, "Wagner_incidentRecordForm_WAGNER0001." The file was last modified on or about June 24, 2008. The document's properties indicate that the author was the first initial combined with the last name of CW1. The document had Tiversa's insignia at the top of the document and was addressed to Wagner. The date of incident was June 24, 2008, and the severity was noted as "Urgent." The document references three documents, "SSN and DOB.rtf" and "ACT SSN DOB.rtf," and WAGNER0001_FILE-LISTING.xls." The incident summary on this Word document noted the following:

> On 6/24/2008, two files were detected being disclosed by what appears to be an internal Wagner Resources employee. The files "SSN and DOB.rtf" and "ACT SSN DOB.rtf" appear to be Wagner Resources internal customer listing documents that contain very sensitive client information (e.g. Customer Names, Social Security Numbers, etc). Upon further investigation of this disclosure source, eighty five additional files were found to be disclosed onto the P2P networks from this same IP address which appears to be COX Communications, Fairfax, VA. ISP. These files also appear to contain internal Wagner Resources information. After performing an initial investigation by reviewing the metadata and the files related to Wagner Resources, Tiversa believes the disclosing source may be a Wagner Resources employee. Tiversa also believes the disclosing computer may be a work computer located within the Wagner Resources internal network. Though other scenarios are possible, based on the current data available, this scenario is the most likely. A more detailed analysis of this disclosure will be conducted as part of Tiversa's Incident Response Case services. The summary information in this ticket is intended to be used by Wagner Resources and Tiversa to investigate and remediate this initial disclosure as quickly as possible while further analysis is underway."

This Incident Record Form was delivered to WRG by Tiversa as part of Tiversa's initial disclosure to WRG of Tiversa's acquisition of WRG's files from the P2P network. Tiversa's allegations of spread were later communicated to WRG after the delivery of this document.

77. The WAGNER0001_FILE_LISTING.xls file was an Excel spreadsheet which appeared to have been authored by the first initial combined with the last name of CW1. The spreadsheet listed approximately 87 files which were inadvertently made available by a WRG employee on a P2P network. All of these files were prepended with the IP address of 70.183.6.112, which was WRG's Fairfax, Virginia, IP address. According to CW1, these files again reflect that Tiversa originally acquired all the WRG files from a WRG employee computer which had a P2P application installed on it, and the other foreign and domestic IP addresses from which Tiversa later claimed to have found the documents were fabricated.

78. The "ACT SSN DOB.rtf" file was last modified on or about June 24, 2008, and did not list an author in the document's properties. According to CW1, he would routinely

remove the author's name prior to sending the document to the client. This file was approximately 154 pages and listed names of WRG clients and the associated PII of those clients, such as date of birth or social security number. One of the individuals listed on this document was Stephen Breyer with an associated social security number. According to public records available to law enforcement, the social security number listed is associated with Supreme Court Justice Breyer.

79. On or about July 9, 2008, Griffin Schultz sent an email to an individual associated with Justice Breyer which appeared to contain text from a Washington Post article dated on or about July 9, 2008. Investigators obtained and reviewed a copy of this article. The article is titled "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing." An internet search confirmed that a Washington Post article was written with the same date and title.

80. According to CW1, Boback called the Washington Post reporters to give them a story which would help generate publicity for Tiversa. CW1 was present during the calls with the Washington Post and Boback gave CW1 updates of such calls during meetings.

81. According to CW1, Boback claimed that he called Justice Breyer and spoke to a staff member, notifying him that Justice Breyer's PII was available on the P2P networks.

82. WRG received a nine-page "P2P Monitoring Status Report" dated January 2010 from Tiversa. Investigators have obtained and reviewed a copy of this Report. The period of time covered was October 1, 2009 to December 31, 2009. The report noted in part that Tiversa was "monitor[ing] global P2P file sharing networks to identify and remediate two sensitive files relating to Wagner Resource Group, Inc: SSN and DOB.rtf [and] ACT SSN DOB.rtf" and "detect[ing] whether these files a) have been re-shared onto the P2P networks by an employee of

Wagner Resource Group, Inc or b) have been downloaded and thus re-shared onto the P2P networks by a third party, such as a supplier, vendor, or cyber criminal." The report further noted in part that, as part of a "File Spread Analysis," "Tiversa's systems detected the files as being downloaded and re-shared by several other individuals utilizing various IP addresses, as indicated below[.]" The report indicated that a file named "ACT SSN DOB.rtf" had "spread" to two IP addresses and that a file named "SSN and DOBs.rtf" had "spread" to 17 IP addresses. According to CW1, the WRG files had not, in fact, "spread" to those other IP addresses; the report was false, and intended to convey to Wagner the importance of maintaining WRG's contract with Tiversa.

83. The report also claimed that, for a total of 19 listed IP addresses, Tiversa had sent a takedown notice to the internet service provider ("ISP"). In fact, according to CW1, he never sent a takedown notice to an ISP associated with an IP address used in the fraud scheme. Keith Tagliaferri and Michael Carulli would have been the only other Tiversa employees to send take down notices. CW1 was not aware of either of these individuals ever sending take down notices for the IP addresses used in the fraud scheme.

OPEN DOOR CLINIC -- PROTECTED HEALTH INFORMATION

84. According to CW1, in about 2008 Tiversa discovered a file on a P2P network containing PII (e.g., SSN, DOB) and PHI, specifically HIV/AIDS test results. CW1 stated that, based on various indicators (e.g., author information in MS Office, and a document containing the company's mission statement), it was determined that these files belonged to Open Door Clinic, a medical facility in Illinois. CW1 stated that, to enhance Tiversa's chances of doing business with Open Door Clinic, Boback instructed CW1 to call patients on the list to inform the patients that

their test results were public. After Open Door Clinic refused to do business with Tiversa, Boback instructed CW1 to manipulate one or more of the files to make it appear as though the files had "spread" over P2P networks, when in fact they had not. Open Door Clinic's Executive Director provided testimony at a Congressional hearing in about July 2014 that an internal investigation of Tiversa's claims revealed no evidence of any Open Door Clinic data leakage on any P2P networks. Moreover, Open Door Clinic could not find any evidence that P2P software was even installed on their network computers. According to Open Door Clinic, they also received a letter from the FTC in 2010 indicating that an Open Door Clinic file had been found on a P2P network. This letter came after Tiversa unsuccessfully attempted to offer its services to Open Door Clinic in 2008 and 2009. I know from CW1, and Tiversa documents I have reviewed, that, during that period, Tiversa was reporting to the FTC companies or entities whose PII or PHI Tiversa claimed to have found on P2P network computers; Open Door Clinic was among the companies Tiversa referred to the FTC. Although Open Door Clinic never became a client of Tiversa, and never found any evidence that any of its PII or PHI had spread over P2P networks, Open Door Clinic nevertheless agreed to a settlement on or about March 7, 2013, to avoid a class action suit brought on by public accusations that Open Door Clinic had disclosed patient data.

## TECHNICAL TERMS

85. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and

includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

b. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security

software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

d. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. "Data Store" is a term used by Tiversa to describe the directory or repository on its servers where Tiversa placed or stored files after downloading them from P2P networked computers.

g. "Information concentrator" is a term used by Tiversa to describe someone who searches P2P networks for sensitive information like PII; the term includes identity thieves.

h. "Spread" is a term used by Tiversa to describe the proliferation of a file or document on P2P networks.

i. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

k. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to set up files on a computer to be shared with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network. However, a tool used by law enforcement restricts the download so that the file is downloaded, in whole or in part, from a single user on the network.

i. When a user wishes to share a file, the user adds the file to his shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

l. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

## COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

86. As described above and in Attachment B, this application seeks permission to search for records and information that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or on other electronic storage media or digital devices. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and

magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and digital devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

87. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found at the SUBJECT PREMISES there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

a. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

b. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer or a smart phone, the data contained in the file does not actually disappear; rather, that data remains on the electronic

storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

88. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence or information that establishes how electronic storage media or digital devices were used, the purpose of their use, who used them, and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be on electronic storage media and digital devices in the SUBJECT PREMISES because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data on the electronic storage media not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage media and digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on electronic storage media or digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how electronic storage media or a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or

absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

89. *Methods To Be Used To Search Digital Devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from electronic storage media also requires specialized tools and often substantial time. As

a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices. In this matter, investigators executing the warrant will attempt to copy some of the digitally stored information, to the extent practicable, while on the SUBJECT PREMISES, [redacted]. However, analysis of the seized data will occur in a controlled, law enforcement environment.

c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic

examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

h. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the SUBJECT PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any electronic storage media or digital devices, as defined above, deemed capable of containing the information, records, or evidence described in Attachment B. To the extent technologically and practically feasible, law enforcement personnel will forensically copy such media and devices on site. Regarding electronic storage media or digital devices that are too large to forensically image in their entirety (e.g., servers), law enforcement personnel may copy files and/or other digital information within the scope of the warrant to law enforcement computer hardware, such as external hard drive(s), in lieu of seizing and transporting such electronic storage media. If such copying on site is not technologically or practically feasible, law enforcement may remove and transport such media and devices to an appropriate law enforcement laboratory or similar facility. Thereafter, law enforcement personnel will review the seized electronic storage media or digital devices, and any copies of the contents of such

media and devices made by law enforcement on the SUBJECT PREMISES in lieu of seizure and removal when technologically and practically feasible, at an appropriate law enforcement laboratory or similar facility. The electronic storage media and digital devices, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel in order to process and analyze the information, records, or evidence described in Attachment B.

2. [redacted]

[redacted]

3. The analysis of the contents of any seized or imaged electronic storage media or digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

4. In searching the seized or imaged electronic storage media or digital devices, the forensic examiners may examine as much of the contents of the electronic storage media or digital devices as deemed necessary to make a determination as to whether the

contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized electronic storage media or digital devices will be specifically chosen to identify only the specific items to be seized under this warrant.

## CONCLUSION

90. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

Mosi K. Forde
Special Agent
U.S. Department of Health and Human Services, Office of Inspector General

Subscribed and sworn to before me on **February 29, 2016:**

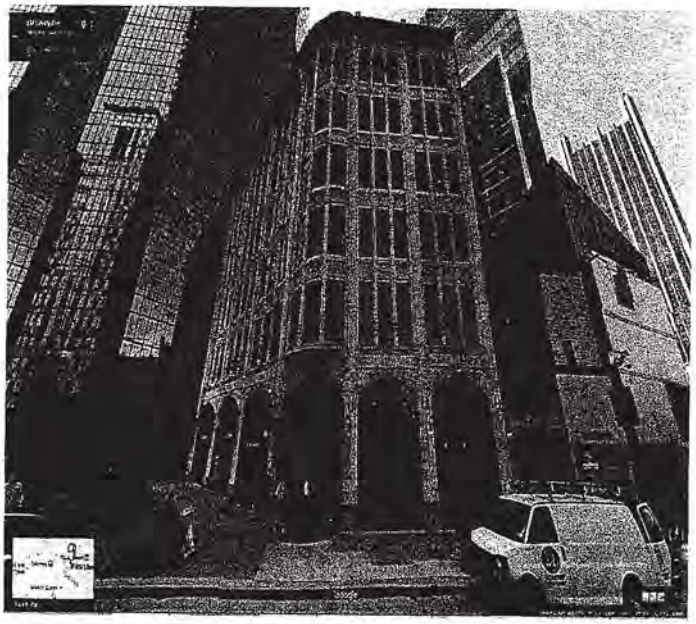
ROBERT C. MITCHELL
UNITED STATES MAGISTRATE JUDGE
**Pittsburgh, PA**

# ATTACHMENT A

*Property to Be Searched*

The property to be searched, that is, the SUBJECT PREMISES are the offices of Tiversa, located on the 2nd, 5th, 6th, and 7th floors of 606 Liberty Avenue, Pittsburgh, PA 15222, the address depicted in the photographs below. That address is a seven-story building. The numbers "606" can be seen at the entrance to the building. Tiversa owns the office building but only operates out of the aforementioned 2nd, 5th, 6th, and 7th floors.

The lobby of the building is located on the 1st floor with a security guard stationed at a desk. Two other businesses lease space on the 1st floor: HealthQuest Chiropratic and Joseph Orlando (a men's clothing store). The 3rd floor is vacant. The entire 4th floor is leased by Celli-Flynn Brennan Architects & Planners. The space leased by businesses other than Tiversa is not considered part of the SUBJECT PREMISES to be searched.




Butcher and The Rye
CVS Pharmacy
Ulrich Shoe Repair
PNC Legacy Project
606 Liberty Ave
Habitat
Moneygram (inside)
Google
Reed Smith LLP
The PNC Financial Services Group, Inc
Radio Hybrid
Starbucks
Sign in

# ATTACHMENT B

***Items to Be Seized***

1. The items to be seized or imaged are evidence, information relating to, fruits, contraband, or instrumentalities of violations of 18 U.S.C. §§ 1349 and/or 371 (Conspiracy to Commit to Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1621 (Perjury), 18 U.S.C. § 1505 (Obstruction of Proceedings), 18 U.S.C. § 1519 (Falsification of Records), and 18 U.S.C. § 1001 (False Statements), as described in the affidavit, including but not limited to the following:

a. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

i. any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa, including but not limited to: LabMD, Transportation Security Administration (TSA), Qualcomm, Renaissance Healthcare (or "Baylor"), Boies Schiller & Flexner, Capitol One, MetLife, Open Door Clinic, Wagner Resource Group, and/or American Express;

ii. any statements or representations made or intended to be made, or records or information produced or intended to be produced, to any government entity concerning Tiversa or Tiversa's work and business practices, including but not limited to any communication with and/or investigation by the Federal Trade Commission or the U.S. House of Representatives, Committee of Oversight and Government Reform; and

iii. any records, documents, and information of any kind reflecting the identities of any coconspirators, accomplices, or aiders and abettors in the commission of the above offenses.

b. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to communications involving any Tiversa employee, officer, director, or agent (including but not limited to email, voicemail, instant messages, Skype chats, and any and all proprietary/internal electronic communication used by Tiversa, such as Spark) where the subject matter of those communications relates to Tiversa's business, including but not limited to

i. Any and all communications that refer or relate to the availability of any client or prospective client's records on any peer-to-peer network;

ii. Any and all communications that refer or relate to Tiversa's discovery of any client or prospective client's records on any peer-to-peer network;

iii. Any and all communications that refer to relate to Tiversa's marketing of its services to any client or prospective client, including but not limited to communications with such client or prospective client or third parties affiliated with clients or prospective clients (such as individuals whose personal identifying information Tiversa purported to have seen made available by a client or prospective client);

iv. Any and all communications that refer to relate to media and/or news coverage of data security breaches in general or Tiversa's services in particular; and

v. Any and all communications that refer or relate to Tiversa's business interest in clients or prospective clients retaining Tiversa's services.

c. All records, documents, and information of any kind (including but not limited to any and all digital information, such as programs, applications, files, logs, and digital communications stored on any electronic storage media or digital devices) that refer or relate to

i. Tiversa's accounting software including but not limited to Peachtree, Sage Software, and/or QuickBooks;

ii. Tiversa's proprietary systems/applications or systems/applications used by Tiversa including but not limited to File Renamer, Eagle Vision, Coveo (or Covio), Ayinger, RAD Importer, FAST, FileDetector, and the Dynamic Signature Profile;

iii. Tiversa's backend databases (e.g., Microsoft Access or SQL/SQLite);

iv. internal/"in-house" Tiversa work products including but not limited to tickets, monthly reports, P2P monitoring status reports, investigation response reports, breach protection reports, Year in Review reports, takedown notices, forensic/forensic investigation reports, and Incident Response Case (or "IRC") reports; and

v. any records in Tiversa's Data Store that refer or relate to any conspiracy or scheme to defraud any and all current or prospective clients of Tiversa.

2. Any and all computers, electronic storage media, or digital devices used in the commission of the above-referenced offenses.

3. All records and logs that refer or relate to the HID Card Reader system installed and housed at SUBJECT PREMISES.

4. All records, documents, programs, applications, and materials that refer or relate to banks and financial institutions, including but not limited to bank statements, passbooks, deposit or withdrawal slips, canceled checks, bank receipts, bank checks, money orders, loan documents, mortgages, safe deposit box keys, credit card records, charge receipts, investment account records and retirement records showing any transfers and/or deposits connected to the offenses outlined above.

5. For any electronic storage media or digital device whose seizure is otherwise authorized by this warrant, and any electronic storage media or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software (and evidence of the lack of such malicious software), as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;

d. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. evidence of the times the COMPUTER was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

l. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.